(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号

特表平9－511606

(43)公表日　平成９年(1997)11月18日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		
Ｇ０６Ｆ	7/58		7522－5Ｅ	Ｇ０６Ｆ	7/58	Ｂ
Ｇ１１Ｂ	20/12	１０２	9295－5Ｄ	Ｇ１１Ｂ	20/12	１０２
	20/18	５４４	9558－5Ｄ		20/18	５４４Ａ
		５７０	9558－5Ｄ			５７０Ｂ
Ｈ０３Ｍ	13/22		8732－5Ｋ	Ｈ０３Ｍ	13/22	

審査請求　未請求　予備審査請求　未請求(全 30 頁)

(21)出願番号　特願平8－523383
(86)(22)出願日　平成８年(1996)１月29日
(85)翻訳文提出日　平成８年(1996)10月１日
(86)国際出願番号　ＰＣＴ／ＩＢ９６／０００７７
(87)国際公開番号　ＷＯ９６／２４０９８
(87)国際公開日　平成８年(1996)８月８日
(31)優先権主張番号　９５２００２４２．６
(32)優先日　1995年２月１日
(33)優先権主張国　オランダ（ＮＬ）
(31)優先権主張番号　９５２００５２０．５
(32)優先日　1995年３月３日
(33)優先権主張国　オランダ（ＮＬ）

(71)出願人　フィリップス　エレクトロニクス　ネムローゼ　フェンノートシャップ
オランダ国　5621　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　1
(72)発明者　ホールマン　ヘンドリク　ドリク　ロデウェイク
オランダ国　5621　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　1
(72)発明者　バッヘン　コンスタント　ポール　マリー　ヨゼフ
オランダ国　5621　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　1
(74)代理人　弁理士　杉村　暁秀　(外６名)

最終頁に続く

(54)【発明の名称】　順列ユニットを含む回路配置及び一団の項目を処理する方法

(57)【要約】
この回路配置は番号の集合の疑似ランダム順列を計算する。該回路配置により計算されることのできる順列は、幾つかの基本的疑似ランダム順列の結合及び計算された順列の逆順列を含むことを要する。（結合とは累積的に繰り返される番号の順序変更に対応し、逆順列とは或る順列を元に戻すところの順列である。）基本的疑似ランダム順列、その結合、及び逆順列はすべて同じ生成器により計算され、該生成器の動作は整係数f_iの或る集合を特定することにより適切な順列を計算することが命令される。該生成器は、αをmのすべての素因数で整除される整数の番号で、もしmが４の倍数ならばαも４の倍数であり、そのポテンシーs(σ)は２以上であるとするとき、Ｉに対応してｎ＝0,…,m-1なる番号ｎの順列σ(n)を計算する。すべての順列に同じαが用いられとき、生成された順列のすべての結合及び逆順列は同じ生成器により同じやり方で計算できると仮定する。第１及び第２の順序はいずれもこのタイプの異なる順列に対応するとし、項目の一団を記憶媒体中に第１の順序で記憶し、該記憶媒体から第２の順序で検索することにより、上記一

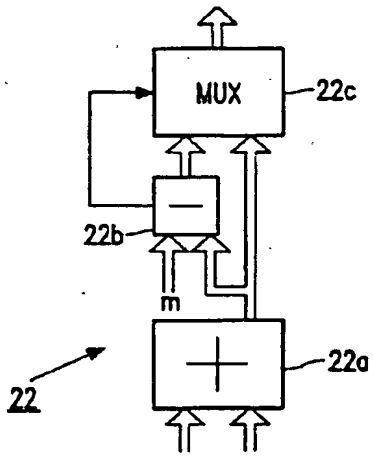

FIG. 4

【特許請求の範囲】

1．一組のm個の番号の逐次疑似ランダム順列を生成する回路配置において、

該回路配置は：

— 制御信号を生成するための制御手段を有して成り、各制御信号は、sを1より大きい自然数とするとき、f_i $(i=0,\cdots,s)$ という(s+1)個の整係数のそれぞれの一組を特定するものであり、また

— 各サイクルが上記制御信号の1つにそれぞれ制御される繰り返しサイクルで動作する計算手段を有して成り、該計算手段は、

f_iを上記制御信号の1つによりそれぞれ特定された整係数とし；αを全サイクルに共通の整数の番号とし、αはmのすべての素因数で整除され且つmに関しsに等しいポテンシーs(α)を持つ；とするとき、

$$\sigma(n) = f_0 + \sum_{i=1}^{s} f_i \left[\frac{n}{\alpha}\right]^{i-1} \bmod m$$

に対応する逐次順列のそれぞれ1つを、上記サイクル中に計算するものであることを特徴とする回路配置。

2．請求項1に記載の回路配置において、

上記制御信号のうち少なくとも1つは、(s+1)個の整係数による順列が、逐次順列のうちから少なくとも2つの順列を結合したものに対応するように、該(s+1)個の整係数を特定することを特徴とする回路配置。

3．請求項1又は2に記載の回路配置において、もしmが4の倍数なら、αも4の倍数であることを特徴とする回路配置。

4．請求項1，2又は3に記載の回路配置において、ポテンシーsは2であることを特徴とする回路配置。

5．請求項1ないし4のうちのいずれか1項に記載の回路配置において、整係数のそれぞれの組のうち少なくとも1つでは、f_0を除くすべてのf_iが互いに等しく且つmとの最大公約数は1であることを特徴とする回路配置。

6．請求項1ないし5のうちのいずれか1項に記載の回路配置において、

上記計算手段は、各サイクル中の逐次順列番号を、中間変数$u^{(i)}$ $(i=0,\cdots$

$,s)$ から、逐次ステップn $(n=0,\cdots,m-1)$で計算するように設定されて成り、

中間変数$u^{(0)}$は、各サイクルの始めのステップの最初の1つで、初期化してf_0とされ、

中間変数$u^{(i)}$ $(i=1,\cdots,p-1)$ は、上記ステップの最初の1つで、初期化して

$$u^{(i)} = f_i \alpha^{i-1}$$

とされ、

$u^{(s)}$を除く各中間変数$u^{(i)}$の値は、上記ステップの最初の1つを除く各逐次ステップで、先行ステップ中の中間変数のそれぞれのモジュロ和

$$u^{(i)} + u^{(i+1)} \bmod m$$

によって置き換えられ、

逐次ステップn $(n=0,\cdots,m-1)$における中間変数$u^{(0)}$の値は、順列置換された番号σ(n)として用いられる

ことを特徴とする回路配置。

7．請求項6に記載の回路配置において、

各々がそれぞれのメモリエレメント及びそれぞれのモジュロ加算器を含むs個の再帰ユニットを縦つなぎに有して成り、

縦つなぎの先頭の再帰ユニットの上記それぞれのモジュロ加算器は、該先頭の再帰ユニットのそれぞれのメモリエレメント及びもう1つ別のメモリエレメントに結合する1目の被加数入力を持ち、

先頭の再帰ユニットを除く各特定の再帰ユニットの上記それぞれのモジュ[redacted]加算器は、該特定の再帰ユニットのメモリエレメントに結合する1番目の被加数入力と、縦つなぎの中で該特定の再帰ユニットの1つ前の再帰ユニットのメモリエレメントに結合する2番目の被加数入力と、を持ち、

各再帰ユニット中のそれぞれのモジュロ加算器の総和出力は、該再帰ユニットのそれぞれのメモリエレメントの入力に接続され、

上記計算手段は、縦つなぎの最終の再帰ユニット中のメモリユニットの内容を各サイクルの始めに初期化してf_0し、また、縦つなぎの最終の再帰ユニッ

トに順次先行する再帰ユニット中のメモリユニットの内容をそれぞれ初期化して

$f_i \alpha^{i-1}$ $(i=1, \cdots, s-1)$

とするように設定され、

もう1つ別のメモリユニットは初期化して$f_s \alpha^{s-1}$とされ、

逐次ステップn (n=1, …, m)では毎回、最終の再帰ユニットのメモリユニットが、ランダム番号σ(n)をその逐次ステップで出力する

ことを特徴とする回路配置。

8．請求項1ないし7のうちのいずれか1項に記載の回路配置において、

メモリを有して成り、m個の番号の組に属するところの番号は該メモリ中のそれぞれの位置を表すアドレスに対応し、また

各特定のサイクルでそれぞれ一組のデータ項目をメモリに書き込み、該特定のサイクルに後続する逐次サイクルの1つで上記それぞれ一組のデータ項目をメモリから読み出すための読み出し／書き込みユニットを有して成り、上記それぞれ一組のデータ項目はその特定サイクル用に生成された順列に対応するアドレスの順番で書き込まれ、後続サイクル用に生成された順列に対応するアドレスの順番で読み出される

ことを特徴とする回路配置。

9．請求項8に記載の回路配置において、上記特定サイクル用に計算された順列の逆順列と上記後続サイクル用に計算された順列との結合が、該特定サイクルとは独立の通常の順列に等しくなるように、整係数f_iの組が選定されること　を特徴とする回路配置。

10．請求項8又は9に記載の回路配置において、符号器を含み、該符号器は上記一組のデータ項目を誤り防護符号で構築するものであることを特徴とする回路配置。

11．請求項8又は9に記載の回路配置において、誤り訂正器を含み、該誤り訂正器は、上記のデータ項目にそれが読み出された順序で与えられた誤り防護符号に従って上記一組のデータ項目を訂正するものであることを特徴とする回路配置。

12．m個の項目の一団を処理する方法であって、

－　該一団の各項目がその一団中の第1順位番号に従って受け取られるところの該一団を受け取る段階、

－　各特定の項目に、該特定の項目の上記第1順位番号の第1関数に従って、記憶媒体内のそれぞれの位置を割り当てる段階、

－　各特定の項目を、記憶媒体内でそれに割り当てられたそれぞれの位置に記憶する段階、

－　第2順位番号を、記憶位置の第2関数に従って各記憶位置に割り当てる段階、

－　記憶媒体から項目を検索する段階、及び

－　特定の記憶位置から検索された上記特定の項目を、該特定の位置の第2順位番号に従って処理する段階

を含んで成る方法において、

n1を順位番号とし；n2を記憶位置の順序での記憶位置の位置番号とし；f_i及びg_i　$(i=0, \cdots, s)$　を各々が(s+1)個の整数から成るそれぞれの集合に属する整係数とし：αをmのすべての素因数で整除される整数の番号とし、αはmに関しsに等しいポテンシーを持つとするとき、上記第1関数及び第2関数はそれぞれ

$$location(n1) = f_0 + \sum_{i=1}^{s} f_i \left[\frac{n1}{1}\right] \alpha^{i-1} \mod m$$

$$ranknumber(n2) = g_0 + \sum_{i=1}^{s} g_i \left[\frac{n2}{1}\right] \alpha^{i-1} \mod m$$

に対応して計算されることを特徴とする方法。

13．請求項12に記載の方法において、もしmが4の倍数なら、αも4の倍数であることを特徴とする方法。

14．請求項12又は13に記載の方法において、ポテンシーs(σ)は2であることを特徴とする方法。

15．請求項12，13又は14に記載の方法において、f_0を除くすべてのf_iが互いに等

しく且つmとの最大公約数は１であることを特徴とする方法。

16. 請求項12ないし15のうちのいずれか１項に記載の方法において、

各サイクル中で逐次順列置換される番号s(σ)は、中間変数$u^{(i)}$ (i＝0, …, s) から、逐次ステップn (n=0, …, m-1)で計算され、

中間変数$u^{(0)}$は、各サイクルの始めのステップの最初の１つで、初期化してf₀とされ、

中間変数$u^{(i)}$ (i＝1, …, p-1) は、上記ステップの最初の１つで、初期化して

$$u^{(i)}=f_i\,\alpha^{i-1}$$

とされ、

$u^{(0)}$を除く各中間変数$u^{(i)}$の値は、上記ステップの最初の１つを除く各逐次ステップで、先行ステップ中の中間変数のそれぞれのモジュロ和

$$u^{(i)}+u^{(i+1)} \bmod m$$

によって置き換えられ、

逐次ステップn (n=0, …, m-1)における中間変数$u^{(0)}$の値は、順列置換された番号σ(n)として用いられる

ことを特徴とする方法。

【発明の詳細な説明】

順列ユニットを含む回路配置及び一団の項目を処理する方法

本発明は、一組のm個の番号の逐次疑似ランダム順列(successive pseudo rando mpermutations)を生成する回路配置に関する。

疑似ランダム順列は種々の用途を持つ。それは、誤り訂正符号と組み合わせてインターリービングの目的で用いることができ、それにより符号からのシンボルを処理する順番を変えて、システマティックな誤りに対し更に強固な誤り防護プロセスとするのである。

単数又は複数の同じ基本的疑似ランダム順列の様々な結合(compositions)により、引き続く幾つかの異なる疑似ランダム順列を生成することが望ましい、という場合はしばしばある。

例えば、もし一組の項目の順序を変えたいと欲するなら、先ずそれらの項目を記憶媒体内の記憶位置に或る順番で書き込み、次にそれらを前と異なる記憶位置の順番で記憶媒体から取り出すのである。複数の組の項目の順序変更を引き続いて行わなければならないときに記憶スペースを節約するため、先行の組が完全に読み出される以前にでも、前の組の項目が検索されて空きになった順序で、それらの記憶位置に後の組の項目を毎回記憶させたい。各組が同じ疑似ランダム順列を用いて順序を変えなければならないなら、これは、引き続く各組を記憶する記憶位置の順序が前の組の記憶位置の順序にその疑似ランダム順列を結合したものでなければならない、ということを意味する。

上記回路配置は、これらの逐次疑似ランダム順列を生成しなければならない。しかし、すべての必要な疑似ランダム順列を生成することは、極めて複雑な時間の掛かる演算を要求されることになろう。生成することのかなり簡単な基本的疑似ランダム順列を用いる場合といえども、そのような基本的疑似ランダム順列の結合を生成することの必要性は、種々の疑似ランダム順列の計算がその複雑さにおいて大幅に異なり、計算時間や所要のハードウェアの極めて高価なことが明らかになるであろうことを意味する。

とりわけ、本発明の目的は、単数又は複数の同じ基本的疑似ランダム順列の結

合である複数の疑似ランダム順列を生成できる回路配置を提供することであり、この回路配置は、一連の同じ計算ステップを実行するのに使われる同じ計算回路を用いて、これらの疑似ランダム順列の各々を生成することができ、必要な計算回路は簡単な構造のものである。

本発明のもう１つの目的は、項目を処理する順番が、項目を受け取る順番の疑似ランダム順列となるような、項目を処理する方法を提供することであって、該順列は項目を記憶媒体に記憶し、記憶媒体から検索することにより達成され、所要の記憶媒体は減らす、というものである。

本発明による回路配置は、

— 制御信号を生成するための制御手段を有して成り、各制御信号は、ｓを１より大きい自然数とするとき、f_i （$i=0,\cdots,s$）という(s+1)個の整係数のそれぞれの一組を特定するものであり、また

— 各サイクルが上記制御信号の１つにそれぞれ制御される繰り返しサイクルで動作する計算手段を有して成り、該計算手段は、

f_iを上記制御信号の１つによりそれぞれ特定された整係数とし；αを全サイクルに共通の整数の番号とし、αはmのすべての素因数で整除され且つmに関しｓに等しいポテンシーs(α)を持つ；とするとき、

$$\sigma(n) = f_0 + \sum_{i=1}^{s} f_i \left[\frac{n}{t}\right] \alpha^{i-1} \mod m$$

に対応する逐次順列のそれぞれ１つを、上記サイクル中に計算するものであることを特徴とする。数αのmに関するポテンシーs(α)とは、

$$\alpha^s = 0 \mod m$$

となる最小の自然数と定義される、すなわちαのｓ乗冪がmで整除される最小の自然数のことである。

本発明は、本発明により生成される順列σ(n)が数学的概念における「群」を形成する、という認識に立脚する。このことは、もし或る基本的疑似ランダム順列が、その各々を一組の整係数f_iで特定することにより、このやり方で計算できるとしたら、その場合にはこれらの基本的疑似ランダム順列のすべての結合、

及びその逆順列さえもが、その各々を整係数f_iの別のそれ自身の組で特定することにより計算できる、ということを意味する。

本発明はこの認識を利用する計算手段を設けて、この計算手段により所与の公式(formula)に対応する順列を計算し、また、整係数f_iの他の組の特定を毎回制御して、他の順列を計算するのに該計算手段を再使用する。こうして、ある範囲の順列と、それらの結合と、それらの逆順列とが、同一の計算手段で順次計算できる。

本発明による回路配置の一実施例では、上記制御信号のうち少なくとも１つは、(s+1)個の整係数による順列が、逐次順列のうちから少なくとも２つの順列結合したものに対応するように、該(s+1)個の整係数を特定する。

本発明による回路配置の一実施例では、ポテンシーｓは２である。このやり方で計算手段の複雑さを最小のものとしてもなお、疑似ランダム順列を合理的に生成できる。しかし更によいランダム性を考慮するならば、更に高いポテンシー、例えば３以上の（４，５等）ポテンシーが好適な場合もあろう。

本発明による回路配置の一実施例では、整係数のそれぞれの組のうち少なくとも１つでは、f_0を除くすべてのf_iが互いに等しく且つmとの最大公約数は１であることを特徴とする。これにより、選択することの特に容易な（f_0は任意である）基本的順列が提供される。このやり方で生成された順列のそれ自身による結合〔σ(σ(n))，σ(σ(σ(n)))等々〕に対応する更に多くの順列、及びこの順列の逆順列が求められる。一般的には、このやり方で求められた順列は、このように簡単な係数f_iの組で特定されないであろう。従って係数f'_iで特定される等しくない他の順列が、少なくとも１つのこのそれぞれの順列の組に関連して使われることになろう。

本発明による回路配置の一実施例では、上記計算手段は：各サイクル中の逐次順列番号を、中間変数$u^{(i)}$（$i=0,\cdots,s$）から、逐次ステップn（$n=0,\cdots,m-1$）で計算するように設定されて成り；中間変数$u^{(0)}$は、各サイクルの始めのステップの最初の１つで、初期化してf_0とされ；中間変数$u^{(i)}$（$i=1,\cdots,p-1$）は、上記ステップの最初の１つで、初期化して

$$u^{(i)} = f_i \alpha^{i-1}$$

とされ；$u^{(s)}$を除く各中間変数$u^{(i)}$の値は、上記ステップの最初の１つを除く各逐次ステップで、先行ステップ中の中間変数のそれぞれのモジュロ和

$$u^{(i)} + u^{(i+1)} \bmod m$$

によって置き換えられ；逐次ステップn (n=0, …, m-1)における中間変数$u^{(0)}$の値は、順列置換された番号σ(n)として用いられる；ことを特徴とする。このやり方で、順次に順列置換された値σ(n)の計算に掛け算を必要としないで、順列を計算することができる。掛け算を実行する回路は複雑で時間の掛かるものだから、このことは順列の計算を更に簡単で速いものとする。

本発明による回路配置のもう１つの実施例では、該回路配置は：各々がそれぞれのメモリエレメント及びそれぞれのモジュロ加算器(modulo adder)を含むｓ個の再帰ユニット(recursion units)を縦つなぎに有して成り；縦つなぎの先頭の再帰ユニットの上記それぞれのモジュロ加算器は、該先頭の再帰ユニットのそれぞれのメモリエレメント及びもう１つ別のメモリエレメントに結合する１番目の被加数入力を持ち；先頭の再帰ユニットを除く各特定の再帰ユニットの上記それぞれのモジュロ加算器は、該特定の再帰ユニットのメモリエレメントに結合する１番目の被加数入力と、縦つなぎの中で該特定の再帰ユニットの１つ前の再帰ユニットのメモリエレメントに結合する２番目の被加数入力と、を持ち；各再帰ユニット中のそれぞれのモジュロ加算器の総和出力は、該再帰ユニットのそれぞれのメモリエレメントの入力に接続され；上記計算手段は、縦つなぎの最終の再帰ユニット中のメモリユニットの内容を各サイクルの始めに初期化してf_0とし、また、縦つなぎの最終の再帰ユニットに順次先行する再帰ユニット中のメモリユニットの内容をそれぞれ初期化して

$$f_i \alpha^{i-1} \quad (i=1, \cdots, s-1)$$

とするように設定され；もう１つ別のメモリユニットは初期化して$f_s \alpha^{s-1}$とされ；逐次ステップn (n=1, …, m)では毎回、最終の再帰ユニットのメモリユニットが、ランダム番号σ(n)をその逐次ステップで出力する；ものとする。

一組のデータ項目を、或る順番でメモリに書き込み、続いてそれらを別の順番でメモリから読み出すことによる疑似ランダム順列に対して、本発明は特に有用

である。このやり方で幾つかの組を順列置換しなければならないときは、メモリ内の１つの組からのデータ項目は、それが読み出されるのに伴って新しい組のデータ項目と置き換えられる。この場合には、毎回基本的順列の結合を生成することによりメモリに対するアドレスを生成する必要が生じる。上記計算手段はこの目的に極めて適している。従って、本発明による回路配置の一実施例では、メモリを有して成り、m個の番号の組に属するところの番号は該メモリ中のそれぞれの位置を表すアドレスに対応し、また、各特定のサイクルでそれぞれ一組のデータ項目をメモリに書き込み、該特定のサイクルに後続する逐次サイクルの１つで上記それぞれ一組のデータ項目をメモリから読み出すための読み出し／書き込ユニットを有して成り、上記それぞれ一組のデータ項目はその特定サイクル用に生成された順列に対応するアドレスの順番で書き込まれ、後続サイクル用に生成された順列に対応するアドレスの順番で読み出されることを特徴とする。

本発明による回路配置の一実施例では、上記特定サイクル用に計算された順列の逆順列と上記後続サイクル用に計算された順列との結合が、該特定サイクルとは独立の通常の順列に等しくなるように、整係数f_iの組が選定される。このやり方で各組内のデータ項目は同じ疑似ランダム順列により順列置換される。

データ項目の疑似ランダム順列は、誤り防護符号と組み合わせて使用するならば、特に有用である。このやり方は、送出又は記憶されようとするデータ項目であって、後に受信又は検索されようとするデータ項目が、誤りに対して強固であることを許容する。

本発明はまた、m個の項目の一団を処理する方法を提供し、該方法は：該一団の各項目がその一団中の第１順位番号に従って受け取られるところの該一団を受け取る段階；各特定の項目に、該特定の項目の上記第１順位番号の第１関数に従って、記憶媒体内のそれぞれの位置を割り当てる段階；各特定の項目を、記憶媒体内でそれに割り当てられたそれぞれの位置に記憶する段階；第２順位番号を、記憶位置の第２関数に従って各記憶位置に割り当てる段階；記憶媒体から項目を検索する段階；及び、特定の記憶位置から検索された上記特定の項目を、該特定の位置の第２順位番号に従って処理する段階；を含んで成る方法であって、更に該方法は、n1を順位番号とし；n2を記憶位置の順序での記憶位置の位置番号とし

；f_i及びg_i（$i=0, \cdots, s$）を各々が(s+1)個の整数から成るそれぞれの集合に属する整係数とし；αをmのすべての素因数で整除される整数の番号とし、αはmに関しsに等しいポテンシーを持つとするとき、上記第１関数及び第２関数はそれぞれ、

$$location(n1) = f_0 + \sum_{i=1}^{s} f_i \binom{n1}{1} \alpha^{i-1} \mod m$$

$$ranknumber(n2) = g_0 + \sum_{i=1}^{s} g_i \binom{n2}{1} \alpha^{i-1} \mod m$$

に対応して計算されることを特徴とする。

この方法によれば、項目の順番は、記憶媒体を使用することにより順列置換がなされ、それらの項目は記憶媒体内のそれらの位置に従って取り扱われる。種々の異なる順列と、それらの結合と、それらの逆順列とは、同じαに対する上記公式を共に満足させる２つの異なる順列に従って、それぞれ記憶し検索することにより、容易に実現できる。茲でいう項目とは例えばデータ項目であるが、他の物理的項目、例えば製造工程中の製品であって、システマティックな製造過程の影響を排除しようと欲するときにも適用できるであろう。それは例えば１つの工程から来る半製品を、利用可能な組立て装置のうちの１つに、システマティックに結び付けることを防止しようと欲するとき等である。

以下に、図面を引用して本発明及びその利点を詳細に説明する。

図１は、順列ユニットを示す図である。

図２は、伝送システムを示す図である。

図３は、アドレス生成器を示す図である。

図４は、モジュロ加算器を示す図である。

図１は、本発明による回路配置用の順列ユニットを示す。この順列ユニットは入力１と出力２とを有し、これらはいずれも読み出し／書き込み手段３に結合する。この読み出し／書き込み手段３はメモリ５に結合する。上記順列ユニットは

更にアドレス生成器７も有し、それはメモリ５のアドレス入力に結合する。

この順列ユニットはクロック（図示されていない）の制御の下に動作する。各クロックサイクルの間に、読み出し／書き込み手段３は、メモリ５から、すなわち当該サイクル用にアドレス生成器７の生成したアドレスを持つ位置から、１つのデータ項目を読み出す。引き続いて読み出し／書き込み手段３は、当該サイクル用に入力１で受け取ったデータ項目を、この位置に書き込む。

その次のクロックサイクルの間には、メモリ５に対し別のアドレスについてこれが繰り返される。こうして、メモリ５の各位置からそれぞれのデータ項目が逐次読み出されて、出力２に与えられる。これらのデータ項目が一緒になって出力２上のデータ項目のブロックを構成する。更にまた、入力上で受け取ったブロック中の各データ項目が、メモリのそれぞれの位置に書き込まれる。

これが引き続くブロックについて繰り返され、アドレス生成器７はメモリの全アドレスを生成する。こうして、各ブロックは逐次メモリに書き込まれ、再びメモリから読み出される。アドレス生成器はこれらのアドレスを自分自身の順序で生成する。従って各ブロックのデータ項目は、書き込まれたときの序列とは異なる序列で読み出される。

この順列ユニットは、例えば誤り防護符号を用いる伝送システムでインターリーブ器(interleaver)又はデインターリーブ器(deinterleaver)として、使用される。

図２はそのような伝送システムを示す。このシステムは符号器10、インターリーブ器12、変調器14、伝送チャネル、復調器16、デインターリーブ器18、及び復号器20を含む。

動作中にデータは符号器10の入力に与えられる。符号器はこれらのデータを誤り訂正符号で符号化する。すべての既知の誤り訂正符号が、例えば畳み込み符号又はターボ符号(turbo code)が、この目的に使用できる。符号化されたデータはブロックに分割されて、その各々がシンボルの論理系列(logic succession)を含む。

復号器20は符号器に対応するもので、符号器10から復号器20への伝送中に生じ

たシンボル誤りを訂正する。誤り訂正符号は論理系列内に亙り分散して生じるシンボル誤りを適切に訂正できるものである。バースト誤り、すなわち論理系列中の多数の連続したシンボルが正しくないという誤りについては、寧ろたやすく訂正し難い。

変調器14は、同時に送出される多数の周波数チャネルを持つ信号を生成する。各ブロックのシンボルは多数のグループに更に分割される。各グループは１つの周波数チャネルに対応し、１グループ内の複数のシンボルの情報は、対応する周波数チャネルで伝送される。このことは、例えば各グループのシンボルを１つの番号として翻訳し、これらの番号を１つの数列に並べて、この数列のFFT(高速フーリエ変換)を形成することにより、実現できる。次いでこのFFT の結果は伝送チャネル、例えば無線地上放送チャネル、を介して送出される。このFFT 変換及び送出は後続のブロックに対し繰り返される。このことはそれ自身既知のOFDM（直交周波数分割マルチプレクシング）技術に対応する。

復調器16は変調器14に対応する。復調器は種々の周波数チャネルを同時に受信して、その各々がそれぞれの周波数チャネルで送られて来たシンボルのグループを再構築する。OFDM技術によれば、受信した信号の逆FFT を形成し、番号を再構築し、それからグループを再構築することにより、このことは実現される。インターリーブ器12は、論理系列内で互いに直接前後して並んだシンボルが殆ど常に異なる周波数チャネルで変調される、ということを保証するのに使われる。これらのチャネル（中間周波数のチャネルについて云えば）は０より寧ろ大きいことが、従って隣のシンボルが隣のチャネルではない処に入るようにするのが好適である。このことは、１つのチャネル又は隣合った複数のチャネルが崩壊しても論理系列中にバースト誤りを引き起こさないことを保証するのに役立つ。

デインターリーブ器18はインターリーブ器12に対応するもので、逆動作を行うことにより論理系列が、復号器20に与えられる前に（シンボル誤りを除いて）順番を再構築される。

インターリーブ器12は、論理系列中で互いに並んでいる各１対のシンボルを、

複数のチャネルの距離だけそれぞれ互いに離して配列する。これらの距離はその

値がそれぞれ異なり、異なる距離は近似的に等しい頻度で起きることが保証されている。その結果、周波数チャネルの周期的システムで低品質の受信につながる伝送チャネルの崩壊に抵抗し得る。（茲で周期的システムとは、低品質の受信が周波数の関数として毎回同数のチャネルの後でそれ自身反復するシステムを意味するものと理解する。）

それ以外の各１対のシンボルで、そのような１対のシンボル中の同時誤りがバースト誤り訂正の問題を起こし得るような互いにかなり接近しているシンボル対は、やはり複数のチャネルの距離だけそれぞれ互いに離して配列する。これらの距離もやはりその値がそれぞれ異なるのが好適であり、異なる距離はやはり等しい頻度で起きることが保証される。

伝送チャネルは実例を用いて示される。本発明から逸脱することなく他のチャネル変調技術を用いることもできよう。

順列群Λα

アドレス生成器７により各ブロックに対しメモリ５のアドレスがその中に生成されるところのそれぞれの数列(sequences)は、各ブロックのデータ項目の順序をどのようにして入れ換えるかを定める。本発明は、mを１つのブロック中のデータ項目の数とし、σ(i)は異なるiに対しては互いに異なるとするとき、数列（σ(0), σ(1), …, σ(m-1)）中のアドレスσ(i)を利用する。このような数列を順列と称し、σという記号で表す。本発明は、二項係数：

$$\binom{n}{i} = \frac{n(n-1)\cdots(n-i+1)}{i!}$$

を用いて、Λαを

$$\Lambda_\alpha = \{ (\sigma(0),\sigma(1),\ldots\sigma(m-1)) \mid \sigma(n) = f_0 + \sum_{i=1}^{s} f_i \binom{n}{i} \alpha^{i-1} \mod m \}$$

と定義するとき、集合Λαの一部を形成する順列σを特に顕著に利用する。茲で

αは、mの任意の素因数で整除され、またmが４で整除されるならば４でも整除されるように選定する。例えばmが100(素因数は２と５)とすれば、αは20の任意の倍数とすることができる。sはαの「ポテンシー」“potency”すなわち：

$$\alpha^s = 0 \mod m$$

となる最小の自然数である。従って上の例では、α＝20であれば、$\alpha^2 = 400$はm＝100で整除されるから、sは2である。αがmのすべての素因数を1回だけ含むならば、そのときこのαは可能な限り最大のポテンシーsを持つ。そのポテンシーはmの素因数のうちで最大の冪を持つ素因数の冪の値に等しい。例えば、m＝45＝3*3*5, α＝15＝3*5とするとき、最高のポテンシーs＝2を持つ、それは素因数3がmのうちで最大の冪の値(2)を持つからである。従って、最小でもポテンシーが2のαを求めるためには、mは少なくとも1つの素数の平方で整除されなければならない：素数であるmの値は、ポテンシーが2又はそれより大きいことは許容されないし、異なる素数の積となることも許容されない。それ故にmは、もしポテンシー2を持つαが要求されるならば、例えば1, 2, 3, 5, 6=2*3, 7, 10=2*5等であることはできない。4もやはりポテンシーが2のαを許容しない。

従って、ポテンシーsが1より大きいαの値を、ゆとりをもって選択することができるためには、mは適当に大きな数でなければならず、また多くの異なる素因数を含んでいなければならい。有限のポテンシーを持つすべてのαの値は、基本的なαの値の整数倍になるであろう。この基本的なαの値は、mのすべての素因数の積であり、可能な限り最高のポテンシーを持つ。

数f_iは、集合$\Lambda\alpha$からのσ(i)順列が0からm－1に亙るように選定された自然数である。（例えばすべてのi＞0に対して$f_i = 1$であるか、又はi＞0でmと互いに素すなわちf_iとmの最大公約数が1であるときにf_iはiと独立であり；$f_0 = 0$であるときに、これは線形合同アルゴリズムから求めることのできる順列に対応する。）

集合$\Lambda\alpha$の内部でσ(n)多項式は数列の中のそれらの位置nに従属する。この多項式の次数は$\Lambda\alpha$の内部では最大でもsである。疑似ランダム順列に対してはsは2次又はそれより高次であることが好適である。ランダム性は、種々の異なる順列を生成して最も良いものを選定することにより、最適化できる。

茲で集合$A\alpha$のエレメントの積を定義する：順列σとπの積σ○πとは、順列σと順列πとの結合である。すなわち

$$(\sigma \circ \pi)(n) = \sigma(\pi(n))$$

と定義する。集合$\Lambda\alpha$が、この積○という算法に関して、群を構成する（数学的概念としての「群」を構成する）ことは証明できる。このことは、$\Lambda\alpha$が恒等順列を含むこと（すなわち$f_0 = 0$, $f_1 = 1$, 且つその他のすべての$f_i = 0$）；$\Lambda\alpha$からの任意の2つの順列の結合は$\Lambda\alpha$に属すること；及び、$\Lambda\alpha$の任意の順列に対しその逆順列も$\Lambda\alpha$に属すること；がすべて成り立つことを意味する。（これは、もしmが4で整除されるとαは4で整除されないような$\Lambda\alpha$に対しても成り立つし、またもし$\Lambda\alpha$が順列に限定されなくても成り立つ。）

積σ○πを記述する数f_iの計算は原理的には置換の問題である。順列σと順列πとを、数g_i及び数h_iを用いてそれぞれ次のように表すことにする：

$$\sigma(n) = g_0 + \sum_{i=1}^{s} g_i \left[\frac{n}{1}\right] \alpha^{i-1} \mod m$$

$$\pi(n) = h_0 + \sum_{i=1}^{s} h_i \left[\frac{n}{1}\right] \alpha^{i-1} \mod m$$

そうすると、積（σ○π）は、σ(n)を表す数式に置換π(n)を施すことにより計算できる、すなわち：

$$(\sigma\circ\pi)(n) = g_0 + \sum_{i=1}^{s} g_i \left[\frac{\pi(n)}{1}\right] \alpha^{i-1} \mod m$$

積σ○πを陽関数として表す数式は二項係数を計算することにより求められる。$\Lambda\alpha$が群を構成することから、この陽関数としての表現は、数f_iを自然数とすれば、次のように書き直すことができる：

$$(\sigma\circ\pi)(n) = f_0 + \sum_{i=1}^{s} f_i \left[\frac{n}{1}\right] \alpha^{i-1} \mod m$$

これらの自然数f_iはこの数式から、例えば差分を用いて計算できる。nの関数π（例えば順列）の差分Δπ(n)は

$$\Delta\pi(n) = \pi(n+1) - \pi(n)$$

と定義する。$\Lambda\alpha$から順列置換を反復して施すことにより

$$[\Delta^i \pi(n)]_{n=0} = h_i \alpha^{i-1}$$

が得られ、$\pi(0)=h_0$がやはり成り立つ。同様にして積$\sigma\circ\pi$に対しても

$$[\Delta^i(\sigma\circ\pi)(n)]_{n=0}=f_i\alpha^{i-1}$$

と$(\sigma\circ\pi)(0)=f_0$とが成り立つ。これを積$\sigma\circ\pi$に対する陽関数に適用すると、

数f_iが求められる。従ってm＝100且つα＝20とした実例で、$\sigma(n)$が$g_0=g_1=g_2=1$であるときには$\sigma(0)=1$, $\sigma(1)=2$, $\sigma(2)=23$, …, $\sigma(23)=84$となり、更にそれから、$\sigma(\sigma(0))=2$, $\sigma(\sigma(1))=23$及び$\sigma(\sigma(0))=84$となる。次いでこれから結合$\sigma(\sigma(n))$は$f_0=2$, $f_1=21$, $f_2=2$により特定される。同様にして計算すれば、$\sigma(\sigma(\sigma(n)))$が$f_0=23$, $f_1=61$, $f_2=3$により特定される。

順列σの逆順列πを表す数h_iは、例えば、f_iに対する数式から積$\sigma\circ\pi=e$に対する解を求めることにより求められる。又はその代わりに、$\sigma_1=\sigma$とするときに、$\sigma_n=\sigma\,\sigma_{n-1}$を順次nについて計算して行って$\sigma_n$が恒等順列となるに至る（これが可能なことは群の性質から保証されている）ならば；σ_{n-1}がσの逆順列である。

数f_iから出発すれば、Λ_αからの順列は再帰的(recursive)な手法で簡単に生成できる。

図３は再帰的アドレス生成器を示し、これはαがポテンシーs=2を持つ場合に、Λ_αからの順列を生成するものである。この図では破線で区切ってあるように、このアドレス生成器は２つのセクションA及びBを含む。このセクションAは、第１レジスタ20、第１加算器22、第１初期化器21、及び第１マルチプレクサー23を含む。第１レジスタ20の出力は該アドレス生成器の出力となる。この出力は第１加算器22の入力に結合する。第１加算器22の出力及び第１初期化器21は、第１マルチプレクサー23を介して第１レジスタ20の入力に結合する。

セクションBは第２レジスタ24、第２加算器26、第２初期化器25、及び第２マルチプレクサー27を含む。第２レジスタ24の出力は第１加算器22のもう１つの入力に結合し、また第２加算器26の入力にも結合する。第２加算器26はまた、メモリ28からの入力信号をも受け取る。第２加算器26の出力及び第２初期化器25は、第２マルチプレクサー27を介して第２レジスタ24の入力に結合する。

図４は、モジュロ加算器(modulo adder)の実施例を示す。加算器22及び加算器26はモジュロ加算器として構成される。図４は、２進(binary)加算器22a, 減算器22b, 及びマルチプレクサー22c を示している。モジュロ加算器22の入力は２進加算器22a の入力を構成する。２進加算器22a の出力は減算器22b 及びマルチプレクサー22c に結合する。減算器22b の出力はまた、マルチプレクサー22c にも結合する。減算器22b の（引き算で上の位から借りる）借り出力(borrow output)はマルチプレクサー22c の制御入力に結合する。マルチプレクサーの出力はモジュロ加算器22の出力を構成する。

２進加算器22a は動作中に入力信号の和を計算する。減算器22b はこの和からmを引き算する。もしこの引き算の結果が０より小さければ、マルチプレクサー22c が、上記の和をただ送出する。もし引き算の結果が０より大きければ、減算器が、和ではなくて該引き算の結果を送出する。

図３のアドレス生成器は、データ項目クロック（図示されていない）と同期して動作する；このクロックは、データ項目が読み出され書き込まれると、その都度１パルスを出力する。レジスタ20及び24の内容はこのパルスに応じて更新される。１つのブロック内でn番目のデータ項目を処理している時におけるレジスタ20及び24の内容をu_n及びv_nと記すと、

$$u_{n+1}=u_n+v_n \mod m$$

$$v_{n+1}=u_n+d \mod m$$

が成り立つ。n=0に対するレジスタ20及び24の内容は初期化器21, 25により初期化される。

それから、第１レジスタ20, 第２レジスタ24がf_0, f_1に初期化され、メモリが第２加算器にf_2 αを与えると、アドレス生成器は次の級数：

$$u(n)=f_0+\sum_{i=1}^{s}f_i\left[\frac{n}{\mu}\right]\alpha^{i-1} \mod m$$

を生成するであろう。ポテンシーの高い方のα値を用いるときは、セクションBのような複数のセクションがセクションAとセクションBの間に縦つなぎに(in cascade)配置される。これらのセクションA, B間に縦つなぎに配置されたセクションには、（A, Bも含んで）順番にi＝1, …, s-1と番号が付され、これら種

々のセクション中のレジスタは、$f_i \alpha^{i-1}$という値に初期化される。

$\Lambda\alpha$から順列を生成するのに用いられるもう1つの差分技術は、変形された差分$\Delta\lambda$、すなわち：

$$\Delta\lambda\sigma(n)=\sigma(n+1)-(1+\alpha\lambda)\sigma(n)$$

と定義された$\Delta\lambda$を利用する。もし$\sigma(n+1)$がこの$\Delta\lambda\sigma(n)$の式を用いて計算されようとするなら、掛け算が必要となろう。しかしλを適切に選定すれば、この計算に必要な再帰的なセクションの数は限定される。

順列群$\Lambda\alpha$の応用

$\Lambda\alpha$の群としての性質から、順列の結合により得られた順列は再び$\Lambda\alpha$に属する順列の簡単な形に書ける。本発明は、疑似ランダム順列を実行するための簡単な順列ユニットの構築に、この態様を利用する。

最初の応用は、同じ順列$\pi(n)$を各ブロックで実行しようと意図する順列ユニットに関する。この順列ユニットは所与のブロックのデータ項目を一連のアドレス$\sigma_j(n)$に従って（すなわち先行のブロックのデータ項目が読み出されたシーケンス内に）書き込む。それに続いて順列ユニットは一連のアドレス$\sigma_{j+1}(n)$に従ってデータ項目を読み出す。すると、n番目のデータ項目として書き込まれたデータ項目は、$\pi(n)$番目のデータ項目として読み出されなければならない。これは、もし$\sigma_{j+1}(n)=\pi(\sigma_j(n))$ならば、従って$\sigma_{j+1}=\pi\circ\sigma_j$ならば成り立つ。引き続くブロックの順列に対し、毎回jを増しながらこれが繰り返される。$\Lambda\alpha$からの順列π及びσ_jが用いられればσ_{j+1}も常に$\Lambda\alpha$に属することになろう。その結果、すべてのσ_jが簡単に生成できる。この目的のために、例えば図3に示すアドレス生成器が使用され、又はその代わりに$\Lambda\alpha$からの順列のエレメントに対する陽関数が使用される。

2番目の応用は、引き続くブロックに対し異なる順列$\pi_j(n)$, $\pi_{j+1}(n)$を実行することに関する。そのときは$\sigma_{j+1}(n)=\pi_j(\sigma_j(n))$が成り立っている。もし順列$\pi_j(n)$, $\pi_{j+1}(n)$が共に同じ$\Lambda\alpha$から選ばれているならば、一連のσ_jもまた$\Lambda\alpha$からの順列となり、簡単に生成できる。

反対に、もしσ_j (j=1,…) がすべて1つの集合Λのエレメントとして選ばれ

ているならば、順次ブロックjに対する順列π_j及びその逆順列はそのΛのエレメントであることが保証され、簡単に生成できる。これは例えば、出力2から送出されたデータ項目“n”がどのように順列置換されたかを信号する必要があるとき、すなわちこのデータ項目を入力1が受け取ったときにブロックj内のその位置$\pi_j^{-1}(n)$を信号する必要があるときに、応用できる。$\pi_j^{-1}(n)$がΛのエレメントであるという事実を用いれば、一連の$\pi_j^{-1}(n)$が、nの引き続く値に対して簡単に生成できる。

これは、疑似ランダム順列（αの最高次数に対する係数f_iが0でない）と恒等順列（$\sigma(n)=0,1,\cdots,m-1$）とがσ_jとして交互に使われるときにも当てはまる。（結果として得られる順列π_jが疑似ランダムであるためには、少なくとも1つ置きに順列σ_jが疑似ランダムであることが必要で、すべてのσ_jがランダムであるには及ばない。）適切に選択されたf_iに対して、これは各ブロックにおける引き続くアドレス間の差がほぼ均等に分布するインターリービングをもたらす。僅かに2つの異なる順列のみを使用することはインターリービングを簡単なものにする。

順列$\pi_j(n)$及び順列$\pi_{j+1}(n)$が異なる集合$\Lambda\alpha$及び$\Lambda\alpha'$から選択されるときは、両方を含む$\Lambda\alpha''$が求められることになり、茲ではα''がαとα'の最大公約数を構成し；そうするとα''のポテンシーは$\Lambda\alpha$及び$\Lambda\alpha'$のそれよりも高くなるであろう。するとσ_jを書き込み、読み出すのに必要なシーケンスは$\Lambda\alpha$に属し、従って簡単に生成できる。

シーケンスσ_jを記述する番号$f_i(j)$は、上記の順列の結合を表す陽関数を用いて計算できる。しかし多くの場合にこれらの番号は再帰的に計算できることが判っている。もしαのポテンシーsが2ならば、

$$f_0^{(0)}=c,\quad f_1^{(0)}=b,\quad f_2^{(0)}=e$$

とするときに：

$$f_0^{(i+1)} = f_0^{(i)} + c\, f_1^{(i)} + [c(c-1)/2]\, \alpha\, f_2^{(i)}$$

$$f_1^{(i+1)} = b\, f_1^{(i)} + (b\, c + b(b-1)/2)\, \alpha\, f_2^{(i)}$$

$$\alpha\, f_2^{(i+1)} = \alpha\, e\, f_1^{(i)} + (b\, b + \alpha(\alpha-1)/2)\, \alpha\, f_2^{(i)}$$

が成り立つ（これらの数式はすべてmodulo mとする）。

本発明は図１及び図２に示す回路配置に応用できる。この回路配置は一連のデータ項目のブロックを受け取り、これらのブロックを出力するための順列ユニットを含み、各ブロックのデータ項目は順列置換された形で出力される。茲で順列ユニットは、

― メモリと；

― データ項目をメモリに書き込み、またメモリから読み出すための書き込み／読み出しユニットと；

― データ項目がメモリに書き込まれ、またメモリから読み出された位置のそれぞれのアドレスから成るアドレス列を生成するためのアドレス生成器と；

を含む。該順列ユニットは、一組のメモリ位置のうちそれぞれのアドレス列を持つ各ブロックからデータを読み出し；最初のブロックを除く各ブロックからのデータ項目を、直前のブロックのデータ項目が読み出されたアドレス列の一組の中に書き込む。

この回路配置では、上記アドレス生成器は各ブロックに対してそれぞれのアドレス列を生成するように配置され、該アドレス列では、各nに対しn番目のアドレスが：

mをブロック内のデータ項目の数とし；αをmのすべての素因数で整除され、ポテンシーs(α)は２か又はそれ以上の整数とし；f_i (i＝0, …, s) をブロックが変われば常に変わる自然数とするとき、次の関係式：

$$\sigma(n) = f_0 + \sum_{i=1}^{s} f_i \left\lfloor \frac{n}{\alpha^i} \right\rfloor \alpha^{i-1} \mod m$$

に一致するところの、番号0, …, m-1の順列σ(n)に対応する。

mが４の倍数ならαは４の倍数であることが好適である。また、アドレス生成

器は、アドレス列を生成するための再帰ユニットと、或るブロックに対しアドレス列を生成する前に再帰ユニットを初期化するための初期化手段とを有することが好適である。簡単な順列を得るためには、ポテンシーs(α)は２であり、nはf_0を除きすべてのf_iが等しく且つmとの最大公約数は１であることが好適である。この回路配置の１つの応用では、順列ユニットの動作は各ブロックに対しそれぞれの順列をもたらし、その順列は書き込むときのアドレス列を当該ブロックの読み出すときのアドレス列に関連させ、f_i (i＝0, …, s) はすべてのブロックに対しそれぞれの順列が同一であるように選定されているものである。

本発明が集合Λαの群としての性質から導かれていることは明らかであろう。データ項目のブロックが毎回この集合からの順列に従って順列置換されるときには、そのような動作はデータ項目のブロックをこの集合からの順列と一致するアドレス列内のメモリに毎回書き込み、続いてこの集合からの別の順列と一致してメモリからこれらのデータ項目を読み出すことにより実行できる。もしαが少なくとも２で且つαの非０の最大幕の係数f_iが０でないならば、これらの順列は疑似ランダムな性格を持つであろう。するとアドレス生成の複雑さは常に同じのままである。アドレス生成器は例えば再帰的な回路を用いて実現できる。このやり方で最も簡単な疑似ランダム順列を生成する方法はポテンシー２のαを使うことである、その訳はそのとき順列を生成するのに必要な計算の数が最少だからである。しかし、ポテンシーの更に高いα値、例えばポテンシー３のα値を使うことは、更によいランダム性を更に容易に実現できるから望ましい、という場合もあろう。それは選択の問題である：生成されたアドレス列を試験して、当該の応に必要なランダム性を持つかどうかが判断されることになる。

本発明が、例として示した伝送システム又はもっと一般的にはアドレス生成器に限定されるものではない、ということは明らかであろう。基本的な疑似ランダム順列の結合である幾つかの疑似ランダム順列を生成しなければならない任意の利用分野に本発明は当てはまる。本発明は、図３に示すような同じ基本的生成器を用い、レジスタ23, 27及びメモリ28を各特定の順列を規定する特定の値に初期

化することにより、これら幾つかの順列を生成するのに用いられる。適切にプロ

グラムされたコンピュータを用いてもこれを達成できることは勿論であって、そこでは一組の係数f_iで特定されるような異なる順列を生成するのに同じプログラム符号が用いられる。

本発明はまた、メモリに記憶されたデータ項目に限定されるものでもない。この順列置換の方法は、任意の物理的種類の一団の項目に適用でき、それは該一団の項目を記憶媒体に記憶させ、その記憶媒体中の位置によりそれらの項目の処理の順序を定める。記憶と検索のそれぞれに同じ群Λαの異なる順列を用いる。このことは、記憶媒体から前の一団の項目が完全に検索される前に次の一団の項目を記憶するとき、更に複雑な順列を必要とせずに記憶媒体中のスペースの節約を可能にする。この一団の項目が、送出することにより処理されるデータ項目であってもよいが、例えば製造工程で処理される製品であってもよいのである。

【図１】

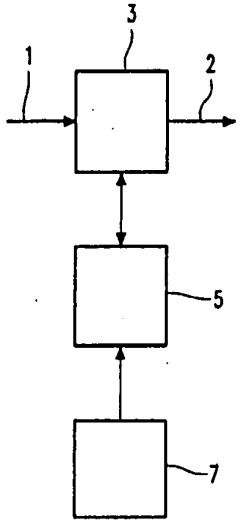

FIG. 1

【図２】

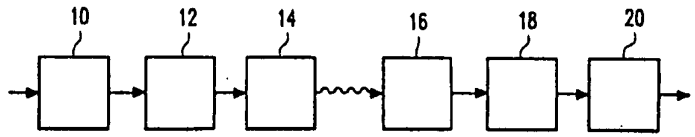

FIG. 2

【図３】

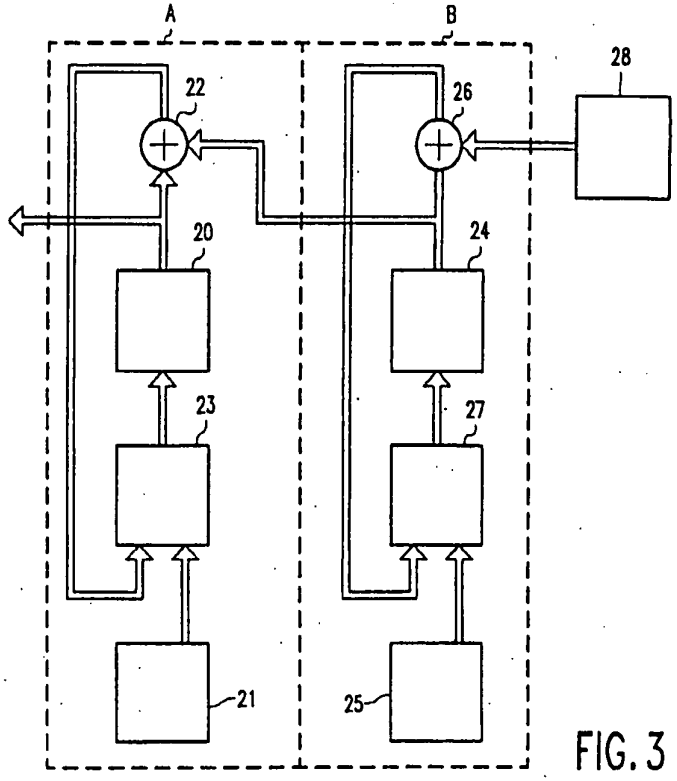

FIG. 3

【図4】

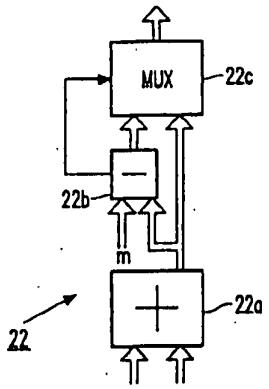

FIG. 4

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 96/00077

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: G06F 7/58
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: G06F, H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0406017 A1 (INDEPENDENT BROADCASTING AUTHORITY), 2 January 1991 (02.01.91), see whole document ---	7-16
Y	US 4547887 A (S.Y. MUI), 15 October 1985 (15.10.85), see whole document --- ---	7-16

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 July 1996	25 -07- 1996
Name and mailing address of the ISA: Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter ɔnal application No.
PCT/IB 96/00077

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [X] Claims Nos.: 1-6
because they relate to subject matter not required to be searched by this Authority, namely:

Rule 39.1

2. [ ] Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. [ ] Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. [ ] As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. [ ] As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest
[ ] The additional search fees were accompanied by the applicant's protest.
[ ] No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet (1)) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

01/07/96

International application No.
PCT/IB 96/00077

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A1- 0406017	02/01/91	AU-A- 5942390	17/01/91
		WO-A,A- 9100672	10/01/91
US-A- 4547887	15/10/85	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(31)優先権主張番号 ９５２００５８０．９
(32)優先日 1995年３月９日
(33)優先権主張国 オランダ（ＮＬ）
(31)優先権主張番号 ９５２００６４２．７
(32)優先日 1995年３月16日
(33)優先権主張国 オランダ（ＮＬ）
(81)指定国 ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＪＰ，ＫＲ

【要約の続き】
団を疑似ランダム的に順列置換し、前の一団が完全にそれから検索されてしまう以前に上記項目の一団を該記憶媒体中に記憶させ始めることを可能にする。